



## **Управление настольными системами**

Профессиональные настольные  
компьютеры

Номер документа: 312947-252

**Сентябрь 2003**

Данное руководство содержит описания и инструкции по использованию средств защиты и технологии Intelligent Manageability, предварительно установленных на некоторых моделях.

© Компания Hewlett-Packard Development (Hewlett-Packard Development Company, L.P.), 2003.

HP, Hewlett Packard и эмблема Hewlett-Packard являются охраняемыми товарными знаками компании Hewlett-Packard в США и других странах.

Compaq и эмблема Compaq являются охраняемыми товарными знаками Hewlett-Packard Development Company, L.P. в США и других странах.

Microsoft, MS-DOS, Windows и Windows NT являются товарными знаками корпорации Microsoft в США и других странах.

Названия прочих изделий или программных продуктов, упомянутые в этом документе, могут являться охраняемыми товарными знаками соответствующих владельцев.

Компания Hewlett-Packard не несет ответственности за технические ошибки или опечатки, которые могут содержаться в настоящем документе, а также за какой-либо случайный или косвенный ущерб, возникший в результате предоставления или использования содержащихся в нем сведений. Сведения в этом документе предоставляются «как есть», без какой-либо гарантии, явной или подразумеваемой, включая все без исключения подразумеваемые гарантии товарности и пригодности для какой-либо определенной цели. Гарантия на продукцию компании Hewlett-Packard предоставляется в прилагаемых к этим изделиям явных заявлениях об ограниченной гарантии. Никакие сведения, содержащиеся в данном документе не должны истолковываться как предоставление дополнительных гарантий.

Представленные в данном руководстве сведения защищены законами, регулирующими отношения авторского права. Никакая часть настоящего руководства не может быть воспроизведена какими-либо средствами (в том числе фотокопировальными) без специального письменного разрешения компании Hewlett-Packard.



**ПРЕДУПРЕЖДЕНИЕ.** Помеченный таким образом текст означает, что несоблюдение рекомендаций может привести к тяжелым телесным повреждениям или гибели человека.

---



**ОСТОРОЖНО!** Помеченный таким образом текст означает, что несоблюдение рекомендаций может привести к повреждению оборудования или потере информации.

---

## **Управление настольными системами**

Профессиональные настольные компьютеры

Вторая редакция (Сентябрь 2003)

Номер документа: 312947-252

---

# Содержание

## Управление настольными системами

Начальная конфигурация и развертывание . . . . .	2
Программа удаленной установки системы. . . . .	4
Обновление и управление программным обеспечением . . . . .	5
Диспетчер HP Client Manager Software . . . . .	5
Решения Altiris . . . . .	6
Служебная программа Altiris PC Transplant Pro . . . . .	7
Диспетчер System Software Manager . . . . .	8
Служебная программа Proactive Change Notification . . . . .	8
ActiveUpdate . . . . .	9
Флэш–ПЗУ . . . . .	10
Удаленное изменение данных флэш–ПЗУ . . . . .	10
Служебная программа HPQFlash . . . . .	11
Аварийный загрузочный блок ПЗУ . . . . .	11
Репликация исходной конфигурации настроек компьютера . . . . .	14
Двухпозиционная кнопка питания . . . . .	25
Узел Интернета . . . . .	26
Объединения и партнеры. . . . .	26
Средства отслеживания и защита. . . . .	27
Защита паролем. . . . .	32
Установка пароля на доступ к программе настройки компьютера с помощью программы настройки компьютера . . . . .	32
Использование пароля на включение питания Программа настройки компьютера . . . . .	33
Встроенная защита . . . . .	38
DriveLock . . . . .	51
Датчик снятия крышки . . . . .	54

Блокировка крышки . . . . .	55
Защита главной загрузочной записи . . . . .	58
Действия, необходимые перед созданием разделов и форматированием текущего загрузочного диска . . . . .	60
Кабельное замковое устройство . . . . .	61
Технология идентификации по отпечаткам пальцев . . . . .	61
Средства уведомления о сбоях и восстановления . . . . .	62
Система защиты диска . . . . .	62
Помехозащищенный блок питания . . . . .	63
Датчик температуры . . . . .	63

## **Указатель**

---

# Управление настольными системами

Технология HP Intelligent Manageability обеспечивает основанные на отраслевых стандартах решения управления настольными компьютерами, рабочими станциями и переносными компьютерами, объединенными в сеть. С введением в производство в 1995 году первых полностью управляемых настольных персональных компьютеров компания Hewlett-Packard стала первооткрывателем в области управляемости настольных систем. Компания Hewlett-Packard получила патент на технологию управления HP Intelligent Manageability и с этого момента Hewlett-Packard является лидером отрасли в области развития стандартов и инфраструктур, необходимых для эффективного проведения работ по развертыванию и настройке настольных компьютеров, рабочих станций и переносных компьютеров, а также управлению ими. Компания Hewlett-Packard работает в тесном сотрудничестве с ведущими компаниями отрасли, предлагающими программные решения по управлению, с целью обеспечения совместимости между системой Intelligent Manageability и этими продуктами. Система управления компьютером Intelligent Manageability является важным элементом выполнения взятых нашей компанией на себя обязательств по обеспечению необходимых на протяжении всего периода службы настольного персонального компьютера решений, помогающих осуществлять контроль на всех четырех фазах рабочего цикла — планировании, развертывании, управлении и переходе.

Система обладает следующими основными средствами и возможностями по управлению настольными компьютерами.

- Начальная конфигурация и развертывание
- Удаленная установка системы

- Обновление программного обеспечения и управления им
- Флэш-ПЗУ
- Средства отслеживания и защиты
- Уведомления о неисправностях и средства восстановления



---

Поддержка особых функций, описанных в этом руководстве, может варьироваться в зависимости от модели или версии программного обеспечения.

---

## Начальная конфигурация и развертывание

Компьютер поставляется с предварительно установленным на нем образом системного программного обеспечения. После непродолжительного процесса «распаковки» программного обеспечения персональный компьютер готов к работе.

Можно заменить предустановленный образ программного обеспечения на пользовательскую настройку системы и программных приложений. Имеется несколько способов развертывания пользовательского образа программного обеспечения. Они включают:

- Установка дополнительных приложений после «распаковки» предварительно установленного образа программного обеспечения.
- Использование программных средств развертывания, таких как Altiris Deployment Solutions™, для замены предустановленного программного обеспечения на пользовательский образ программного обеспечения.
- Использование процесса клонирования дисков, чтобы скопировать содержание с одного жесткого диска на другой.

Выбор наилучшего метода развертывания зависит от особенностей информационно–вычислительной среды и технологических процессов, реализованных на данном компьютере. Сведения, которые могут помочь выбрать наилучший метод развертывания находятся в разделе «PC Deployment» (развертывание ПК), расположенном на веб–узле Lifecycle Solutions (решения, необходимые на протяжении всего периода службы) по адресу: (<http://h18000.www1.hp.com/solutions/pcsolutions>).

Компакт–диск *Restore Plus!*, программа установки на основе ПЗУ и оборудование, поддерживающее стандарт ACPI, обеспечивают помощь по восстановлению системного программного обеспечения, управлению конфигурацией и устранению неполадок, а также управлению электропитанием.

## Программа удаленной установки системы

Программа удаленной установки системы (Remote System Installation) позволяет осуществлять запуск и установку программного обеспечения, используя для этого находящиеся на сетевом сервере программные средства и конфигурационные данные, активируемые с помощью предзагрузочной среды выполнения (PXE, Preboot Execution Environment). Эта функциональная возможность обычно применяется в качестве средства для конфигурирования и установки рабочих параметров системы, и может использоваться для выполнения следующих операций:

- Форматирование жесткого диска.
- Развертывание образа программного обеспечения на одном или нескольких новых персональных компьютерах.
- Удаленное обновление базовой системы ввода–вывода (BIOS) во флэш–ПЗУ ([«Удаленное изменение данных флэш–ПЗУ» на стр. 10](#)).
- Конфигурирование параметров базовой системы ввода–вывода (BIOS).

Чтобы запустить программу удаленной установки системы (Remote System Installation), нажмите клавишу **F12**, когда в нижнем правом углу экрана с эмблемой Hewlett–Packard появится сообщение «F12 = Network Service Boot» (служба загрузки по сети). Далее следуйте инструкциям на экране. В соответствии с порядком загрузки по умолчанию вначале загружаются параметры конфигурации BIOS. Этот порядок может быть изменен для всех последующих попыток на загрузку PXE.

Hewlett–Packard и Altiris, Inc. объединили свои усилия с целью предоставить программные средства, помогающие сделать задачу развертывания и управления ПК на больших предприятиях и фирмах более легкой и требующей меньше времени, значительно снижающие совокупную стоимость владения и превращающие компьютеры Hewlett–Packard в наиболее легко управляемые клиентские компьютеры в корпоративной среде.



## Обновление и управление программным обеспечением

Hewlett–Packard предоставляет несколько средств управления программным обеспечением для настольных компьютеров и рабочих станций и его обновлением: служебные программы Altiris; Altiris PC Transplant Pro; HP Client Manager Software, решение Altiris; System Software Manager; Proactive Change Notification и ActiveUpdate.

### Диспетчер HP Client Manager Software

Диспетчер HP Client Manager Software (HP CMS) обеспечивает тесную интеграцию технологии HP Intelligent Manageability в решения Altiris, предоставляя первоклассные возможности управления оборудованием для устройств доступа Hewlett–Packard. К числу этих возможностей относятся следующие:

- Детальный просмотр перечня оборудования для управления учетом.
- Диагностика и наблюдение за состоянием ПК.
- Заблаговременное уведомление об изменениях в аппаратной среде.
- Сообщение через Интернет о наиболее важных для ведения бизнеса событиях, таких как предупреждения о перегреве компьютеров, об изменениях памяти и т. п.
- Удаленное обновление программного обеспечения, например, драйверов устройств и системы ввода–вывода (BIOS) ПЗУ.
- Удаленное изменение порядка загрузки

Дополнительные сведения о диспетчере HP Client Manager см. на веб–узле [http://h18000.www1.hp.com/im/client\\_mgr.html](http://h18000.www1.hp.com/im/client_mgr.html).

## Решения Altiris

Решения на основе диспетчера HP Client Manager обеспечивают централизованное управление оборудованием клиентских устройств компании Hewlett–Packerd в следующих областях жизненного цикла информационных технологий.

- Управление запасными и основными компьютерными средствами
  - ☐ Соответствие с условиями лицензионного соглашения на программное обеспечение
  - ☐ Отслеживание компьютеров и подготовка отчетов
  - ☐ Отслеживание выполнения условий договора аренды и использования ресурсов
- Развертывание и миграция
  - ☐ Миграция Microsoft Windows 2000 или Windows XP Professional или Windows XP Home Edition
  - ☐ Развертывание системы
  - ☐ Миграция личных настроек
- Справочная служба и устранение неполадок
  - ☐ Управление мандатами справочной службы
  - ☐ Дистанционное устранение неисправностей
  - ☐ Дистанционное разрешение проблем
  - ☐ Восстановление систем клиентов после аварий
- Управления программным обеспечением и операционной средой
  - ☐ Текущее управление настольным компьютером
  - ☐ Развертывание системного программного обеспечения компании Hewlett–Packerd
  - ☐ Применение средств самовосстановления

На некоторых моделях настольных и переносных компьютеров агент системы управления Altiris включается как часть предварительно загруженного образа программного обеспечения. Данный агент обеспечивает связь с программным обеспечением Altiris Development Solutions, которое может использоваться для завершения развертывания нового оборудования или для перемещения индивидуальных настроек в новую операционную систему с помощью простых в использовании мастеров. Решения Altiris предоставляют простые в использовании возможности распространения программ. При использовании этих решений совместно с диспетчером System Software Manager или с диспетчером HP Client Manager Software администраторы могут также обновлять ПЗУ базовой системы ввода-вывода и драйверы устройств с центральной консоли.

Дополнительные сведения можно получить на веб-узле по адресу: <http://www.hp.com/go/easydeploy>.

## **Служебная программа Altiris PC Transplant Pro**

Служебная программа Altiris eXpress PC Transplant Pro позволяет безболезненно производить миграцию с одного ПК на другой с сохранением прежних параметров настройки и данных; при этом осуществляется их быстрый и простой перенос в новую среду. Обновление занимает считанные минуты, а не часы и дни, позволяя настроить настольный компьютер в соответствии с конкретными требованиями пользователей.

Дополнительные более подробные сведения о том, как выполняется загрузка ознакомительной полнофункциональной версии, работоспособной в течение 30 дней, можно получить на веб-узле по адресу: <http://h18000.www1.hp.com/im/prodinfo.html#deploy>.

## Диспетчер System Software Manager

Средство System Software Manager (SSM) является программой, позволяющей обновлять программное обеспечение системного уровня одновременно на нескольких компьютерах. При запуске в системе клиентского ПК средство SSM определяет имеющиеся версии программ и устройств, а затем производит обновление соответствующего программного обеспечения из центрального архива данных, известного также под названием «файловое хранилище». Версии драйверов, поддерживаемых диспетчером SSM, содержащиеся на веб-узле загрузки драйверов и на компакт-диске Support Software (программное обеспечение поддержки), помечены специальным значком. Загрузить эту служебную программу и получить дополнительные сведения о диспетчере SSM можно с веб-странице, расположенной по адресу: <http://h18000.www1.hp.com/im/ssmwp.html>.

## Служебная программа Proactive Change Notification

Программой заблаговременного распространения уведомлений об изменениях (Proactive Change Notification) используется веб-узел Subscriber's Choice, чтобы автоматически и заранее:

- Посылать пользователям по электронной почте уведомления PCN (Proactive Change Notification), заблаговременно (за 60 дней) информируя их об изменениях в оборудовании и программном обеспечении для большинства коммерческих компьютеров и серверов.
- Посылать пользователям по электронной почте сообщения, содержащие выпуски Customer Bulletins, Customer Advisories, Customer Notes, Security Bulletins и Driver Alerts для большинства коммерческих компьютеров и серверов.

Чтобы получать информацию, относящуюся только к своей ИТ-среде, пользователь создает собственный профиль. Получить дополнительные сведения о программе Proactive Change Notification и создать свой собственный профиль можно на веб-узле по адресу: <http://www.hp.com/go/pcn>.

## ActiveUpdate

ActiveUpdate — это клиентское приложение, разработанное компанией Hewlett–Packard. Клиентское приложение ActiveUpdate запускается на локальном компьютере и использует заданный пользователем профиль для заблаговременной автоматической загрузки обновлений программного обеспечения, предназначенных для большинства коммерческих компьютеров и серверов Hewlett–Packard. Эти загруженные обновления программного обеспечения могут быть правильным образом развернуты именно на тех компьютерах, для которых они предназначаются, с помощью диспетчеров HP Client Manager Software и System Software Manager.

Получить дополнительные сведения об ActiveUpdate, загрузить это приложение и создать свой собственный профиль можно на веб-узле по адресу:  
<http://h18000.www1.hp.com/products/servers/management/activeupdate/index.html>.

## Флэш-ПЗУ

Компьютер поставляется с программируемым устройством флэш-ПЗУ (постоянным запоминающим устройством). Для защиты ПЗУ от несанкционированного обновления и перезаписи можно установить пароль в служебной программе настройки компьютера (F10). Это важно для обеспечения надежной работы компьютера. При необходимости обновления данных ПЗУ можно выполнить следующие действия:

- Заказать в компании Hewlett–Packard дискету с обновлением — ROMPaq™.
- Загрузить самые последние образы ROMPaq с веб-узла по адресу: <http://h18000.www1.hp.com/im/ssmwp.html>.



**ОСТОРОЖНО!** Для обеспечения максимального уровня защиты ПЗУ следует убедиться, что установлен пароль для входа в программу настройки компьютера. Этот пароль позволяет предотвратить несанкционированное обновление ПЗУ. Диспетчер System Software Manager позволяет системному администратору установить пароль на одном или нескольких ПК одновременно. Дополнительные сведения см. на веб-узле <http://h18000.www1.hp.com/im/ssmwp.html>.

---

## Удаленное изменение данных флэш-ПЗУ

Возможность удаленного изменения данных флэш-ПЗУ (Remote ROM Flash) позволяет системному администратору безопасно обновлять ПЗУ на удаленных компьютерах Hewlett–Packard непосредственно с центральной консоли управления сетью. Возможность удаленного выполнения этой задачи системным администратором одновременно на нескольких компьютерах позволяет согласовано проводить развертывание образов ПЗУ на находящихся в сети компьютерах Hewlett–Packard и лучше контролировать этот процесс. Это также способствует повышению производительности и снижению затрат на обслуживание.



Для осуществления возможностей удаленного изменения данных флэш-ПЗУ компьютер должен находиться во включенном состоянии или должны быть задействованы средства дистанционного включения компьютера по сети.

Дополнительные сведения об удаленном изменении данных флэш-ПЗУ приводятся в описании диспетчеров HP Client Manager Software и System Software Manager на веб-узле по адресу: <http://h18000.www1.hp.com/im/prodinfo.html>.

## Служебная программа HPQFlash

Служебная программа HPQFlash используется для выполнения локального обновления или восстановления системного ПЗУ на персональном компьютере, работающем под управлением операционной системы Windows.

Дополнительные сведения о служебной программе HPQFlash см. на веб-узле по адресу:  
<http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18607.html>.

## Аварийный загрузочный блок ПЗУ

Аварийный загрузочный блок ПЗУ (FailSafe Boot Block ROM) обеспечивает восстановление системы в случае отказа флэш-ПЗУ, например, при отключении питания во время обновления данных ПЗУ. Загрузочный блок представляет собой защищенный от перезаписи раздел ПЗУ, который при включении питания системы находит флэш-ПЗУ, не содержащее ошибок.

- Если системное ПЗУ не содержит ошибок, компьютер загружается как обычно.
- Если происходит сбой системного ПЗУ при проверке, аварийный загрузочный блок ПЗУ позволяет загрузить систему с дискеты ROMPaq, которая перепрограммирует системное ПЗУ по образцу, не содержащему ошибок.

Когда загрузочный блок обнаруживает повреждение системного ПЗУ, индикатор питания мигает красным цветом 8 раз (один раз в секунду) с последующей двухсекундной паузой. Одновременно с этим подается 8 звуковых сигналов. На экране отображается сообщение о переходе в режим восстановления загрузочного блока (на некоторых моделях).

Чтобы восстановить систему после ее входа в режим восстановления загрузочного блока, сделайте следующие шаги:

1. Если в дисковом для гибких дисков находится дискета, удалите ее и выключите питание компьютера.
2. Вставьте в дисковод для гибких дисков дискету ROMPaq.
3. Включите питание.
4. Если дискета ROMPaq не распознается, будет выведено сообщение о необходимости вставить дискету и перезагрузить компьютер.
5. Если был установлен пароль на вход в программу настройки, загорится индикатор Caps Lock и появится запрос на ввод пароля.
6. Введите пароль на вход в программу настройки.
7. Если система успешно загружается с дискеты и ПЗУ успешно перепрограммируется, на клавиатуре загораются три индикатора. Серия звуковых сигналов повышающегося тона также сообщает об успешном завершении загрузки.
8. Удалите дискету и выключите питание.
9. Опять включите питание, чтобы перезагрузить компьютер.

В следующей таблице представлены различные сочетания световых сигналов индикаторов клавиатуры, используемые загрузочным блоком ПЗУ (когда к компьютеру подсоединена PS/2-клавиатура), а также значение сигналов и необходимые действия.



## Сочетания световых сигналов индикаторов клавиатуры, используемых загрузочным блоком ПЗУ

Режим аварийной загрузки	Цвет светодиодного индикатора на клавиатуре	Клавиатура Действие индикатора	Состояние/сообщение
Num Lock	Зеленый	Включено	Дискета ROMPaq отсутствует, повреждена или дисковод не готов
Caps Lock	Зеленый	Включено	Введите пароль.
Num, Caps, Scroll Lock	Зеленый	Мигание световых индикаторов в последовательности — N, C, SL	Клавиатура заблокирована при работе в сетевом режиме
Num, Caps, Scroll Lock	Зеленый	Включено	Загрузочный блок флэш-ПЗУ успешно завершил работу. Отключите питание и перезагрузитесь
 Диагностические индикаторы не мигают на клавиатурах USB			

## Репликация исходной конфигурации настроек компьютера

Описанные ниже процедуры позволяют администратору легко скопировать исходную конфигурацию настроек компьютера на другой компьютер такой же модели. Это позволяет быстро и эффективно настроить параметры нескольких компьютеров.



Для выполнения обеих процедур необходим дисковод для гибких дисков или поддержка флэш-устройства USB, например HP Drive Key.

---

## Копирование на один компьютер



**ОСТОРОЖНО!** Исходные настройки конфигурации зависят от модели компьютера. Репликация настроек конфигурации с одного компьютера на компьютер другой модели может привести к повреждению файловой системы последнего. Например, нельзя копировать настройки конфигурации с настольного компьютера модели D510 со сверхплоским горизонтальным корпусом на компьютер модели D510 e-pc.

---

1. Выберите исходные настройки конфигурации, которые требуется скопировать. Включите или перезагрузите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузить компьютер**.
  2. Как только индикатор монитора станет зеленым, нажмите клавишу **F10**. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.
- 



Если не нажать клавишу **F10** в нужное время, придется выключать компьютер, потом включать его снова и повторно нажимать клавишу **F10**, чтобы получить доступ к программе.

---

3. Вставьте в дисковод дискету или подсоедините флэш-устройство USB.

4. В меню **File** (файл) выберите пункт **Save to Diskette** (сохранить на дискете). Следуйте инструкциям на экране по созданию дискеты или флэш-устройства USB с настройками конфигурации.
5. Выключите компьютер, на который будут переноситься настройки конфигурации, и вставьте в его дисковод дискету или подсоедините к нему флэш-устройство USB с настройками конфигурации.
6. Включите компьютер, на который будут переноситься настройки конфигурации. Как только индикатор монитора станет зеленым, нажмите клавишу **F10**. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.
7. В меню **File** (файл) выберите пункт **Restore from Diskette** (восстановить с дискеты) и следуйте инструкциям на экране.
8. Перезапустите компьютер после завершения настройки его конфигурации.

## Копирование на несколько компьютеров



**ОСТОРОЖНО!** Исходные настройки конфигурации зависят от модели компьютера. Репликация настроек конфигурации с одного компьютера на компьютер другой модели может привести к повреждению файловой системы последнего. Например, нельзя копировать настройки конфигурации с настольного компьютера модели D510 со сверхплоским горизонтальным корпусом на компьютер модели D510 e-pc.

В описываемом методе процедура подготовки конфигурационной дискеты или конфигурационного флэш-устройства USB займет несколько больше времени, чем в предыдущем случае, однако процесс копирования на целевой компьютер будет осуществляться значительно быстрее.



В операционной системе Windows 2000 отсутствуют средства создания загрузочной дискеты. Однако для выполнения данной процедуры требуется иметь загрузочную дискету или создать загрузочное флэш-устройство USB. Если отсутствует возможность создать загрузочную дискету с помощью Windows 9x или Windows XP, придется использовать описанный выше метод копирования на один компьютер (см. «Копирование на один компьютер» на стр. 14).

---

1. Создайте загрузочную дискету или флэш-устройство USB. См. «Загрузочная дискета» на стр. 17, «Поддерживаемые флэш-устройства USB» на стр. 18 или «Неподдерживаемые флэш-устройства USB» на стр. 22.
- 



**ОСТОРОЖНО!** Загрузка с помощью флэш-устройства USB может выполняться не на всех компьютерах. Если в служебной программе настройки компьютера (F10) указан порядок загрузки по умолчанию, предусматривающий, что попытка загрузки с флэш-устройства предшествует загрузке с жесткого диска, загрузка данного компьютера с флэш-устройства USB может быть произведена. В противном случае необходимо будет использовать загрузочную дискету.

---

2. Выберите исходные настройки конфигурации, которые требуется скопировать. Включите или перезагрузите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузить компьютер**.
  3. Как только индикатор монитора станет зеленым, нажмите клавишу **F10**. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.
- 



Если не нажать клавишу **F10** в нужное время, придется выключать компьютер, потом включать его снова и повторно нажимать клавишу **F10**, чтобы получить доступ к программе.

---

4. Вставьте в дисковод загрузочную дискету или подсоедините загрузочное флэш-устройство USB.

5. В меню **File** (файл) выберите пункт **Save to Diskette** (сохранить на дискете). Следуйте инструкциям на экране по созданию дискеты или флэш-устройства USB с настройками конфигурации.
6. Загрузите служебную программу BIOS репликации настройки конфигурации (repset.exe) и скопируйте ее на конфигурационную дискету или флэш-устройство USB. Эту служебную программу можно получить на веб-узле по адресу:  
<http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18040.html>.
7. Создайте на конфигурационной дискете или флэш-устройстве USB файл autoexec.bat, содержащий следующую команду:  
**repset.exe**
8. Выключите компьютер, на который будут переноситься настройки конфигурации. Вставьте в его дисковод дискету или подсоедините к нему флэш-устройство USB и включите компьютер. Произойдет автоматический запуск служебной программы конфигурации.
9. Перезапустите компьютер после завершения настройки его конфигурации.

## Создание загрузочных устройств

### Загрузочная дискета

---



Приводящиеся ниже инструкции относятся к Windows XP Professional и Windows XP Home Edition. В операционной системе Windows 2000 отсутствуют средства создания загрузочной дискеты.

---

1. Вставьте дискету в дисковод.
2. В меню **Пуск** выберите команду **Мой компьютер**.
3. Щелкните правой кнопкой мыши значок дисковода для гибких дисков и выберите команду **Форматирование**.

4. Установите флажок **Создание загрузочного диска MS-DOS**, а затем нажмите кнопку **Начать**.

Далее см. [«Копирование на несколько компьютеров»](#) на стр. 15.

## Поддерживаемые флэш-устройства USB

На поддерживаемых устройствах, таких как HP Drive Key или DiskOnKey, имеется заранее установленный образ, упрощающий процесс их превращения в загрузочные. Если на используемом устройстве Drive Key такой образ отсутствует, следует использовать процедуру, описание которой также будет приведено в данном разделе (см. [«Неподдерживаемые флэш-устройства USB»](#) на стр. 22).



**ОСТОРОЖНО!** Загрузка с помощью флэш-устройства USB может выполняться не на всех компьютерах. Если в служебной программе настройки компьютера (F10) указан порядок загрузки по умолчанию, предусматривающий, что попытка загрузки с флэш-устройства предшествует загрузке с жесткого диска, то загрузка данного компьютера с флэш-устройства USB возможна. В противном случае необходимо будет использовать загрузочную дискету.

Чтобы создать загрузочное флэш-устройство USB, необходимо иметь:

- Компьютер одной из следующих моделей:
  - ❑ настольный компьютер Compaq Evo D500 со сверхплоским горизонтальным корпусом;
  - ❑ компьютер Compaq Evo D510 модернизируемая модель с вертикальным корпусом/с уменьшенным корпусом;
  - ❑ профессиональные настольные компьютеры HP Compaq d530 следующих серий – со сверхплоским горизонтальным корпусом, с уменьшенным корпусом или модернизируемая модель с вертикальным корпусом;
  - ❑ переносной компьютер Compaq Evo серий N400c, N410c, N600c, N610c, N620c, N800c или N1000c;
  - ❑ переносной компьютер Compaq Presario серий 1500 или 2800.

В зависимости от индивидуальных особенностей системы BIOS будущие модели компьютеров также могут поддерживать загрузку с устройства HP Drive Key.



**ОСТОРОЖНО!** Если используется модель компьютера, не указанная в приведенном выше списке, убедитесь, что в служебной программе настройки компьютера (F10) указан порядок загрузки по умолчанию, предусматривающий, что попытка загрузки с USB-устройства предшествует загрузке с жесткого диска.

- Один из следующих модулей хранения:
  - ☐ 16–мегабайтный модуль HP Drive Key
  - ☐ 32–мегабайтный модуль HP Drive Key
  - ☐ 32–мегабайтный модуль DiskOnKey
  - ☐ 64–мегабайтный модуль HP Drive Key
  - ☐ 64–мегабайтный модуль DiskOnKey
  - ☐ 128–мегабайтный модуль HP Drive Key
  - ☐ 128–мегабайтный модуль DiskOnKey
- Загрузочную дискету DOS с программами FDISK и SYS. Если на ней отсутствует программа SYS, то может использоваться программа FORMAT, однако в этом случае все файлы, имеющиеся на устройстве Drive Key, будут утеряны.
  1. Отключите компьютер.
  2. Подсоедините устройство Drive Key к одному из USB–портов компьютера и отсутствует все другие USB–устройства хранения данных за исключением USB–накопителей для дискет.
  3. Вставьте загрузочную дискету DOS с программами FDISK.COM и SYS.COM (или FORMAT.COM) в дисковод и включите компьютер, чтобы выполнить загрузку с загрузочной дискеты DOS.
  4. Запустите программу FDISK, введя после приглашения A:\ **FDISK** и нажав клавишу ENTER. При выводе на экран соответствующего запроса, выберите **Yes (Y)** (да), чтобы включить поддержку больших дисков.

5. Выберите вариант [5], чтобы отобразить накопители компьютера. Устройству Drive Key будет соответствовать накопитель, емкость которого практически совпадает с его емкостью. Обычно это последний накопитель в отображаемом списке. Запишите букву, соответствующую имени этого накопителя.

Накопитель, соответствующий устройству  
Drive Key drive: \_\_\_\_\_



**ОСТОРОЖНО!** Если емкость накопителя не совпадает с емкостью устройства Drive Key, выполнение описываемой процедуры следует прекратить, поскольку все данные могут быть потеряны. Проверьте все USB-порты на наличие других устройств хранения данных. Если будет обнаружено какое-либо из этих устройств, отсоедините его, выполните перезагрузку компьютера и повторите описываемую процедуру, начиная с шага 4. Если таких устройств не будет обнаружено, то либо данный компьютер не поддерживает устройства Drive Key, либо устройство Drive Key является неисправным. НЕ пытайтесь сделать Drive Key загрузочным устройством.

---

6. Выйдите из программы FDISK, нажав клавишу **ESC**, чтобы вернуться к приглашению A:\.
7. Если на загрузочной дискете DOS имеется программа SYS.COM, переходите к шагу 8. В противном случае переходите сразу к шагу 9.
8. Введите после приглашения A:\ **SYS x:**, где x соответствует букве имени накопителя, записанной нами на шаге 5. Переходите к шагу 13.



**ОСТОРОЖНО!** Убедитесь, в правильности ввода имени накопителя, соответствующего устройству Drive Key.

---

После завершения переноса системных файлов, программа SYS возвратится к приглашению A:\.

9. Скопируйте все необходимые файлы с устройства Drive Key во временную папку на другом диске (например, на внутренний жесткий диск компьютера).



10. Введите после приглашения A:\ **FORMAT /S X:**, где X соответствует букве имени накопителя, записанной нами ранее.



**ОСТОРОЖНО!** Убедитесь, в правильности ввода имени накопителя, соответствующего устройству Drive Key.

Программа FORMAT выведет одно или несколько предупреждений, в которых спрашивается, следует ли продолжать выполнение процедуры. Каждый раз в ответ на них необходимо вводить **y** (да). Программа FORMAT выполнит форматирование устройства Drive Key, добавит на него системные файлы и предложит ввести метку тома.

11. Нажмите клавишу **ENTER**, чтобы отказаться от ввода метки или введите ее, если хотите это сделать.
12. Скопируйте все файлы, сохраненные на шаге 9, обратно на устройство Drive Key.
13. Удалите дискету и выполните перезагрузку компьютера. Компьютер загрузится с устройства Drive Key, которое отобразится в качестве диска C.



Порядок загрузки по умолчанию на различных компьютерах может быть разным, и может быть изменен с помощью служебной программы настройки компьютера (F10).

При использовании версии DOS из Windows 9x, некоторое время может отображаться экран с эмблемой Windows. Если это нежелательно, добавьте файл нулевого размера с именем LOGO.SYS в корневой каталог устройства Drive Key.

Далее см. «Копирование на несколько компьютеров» на стр. 15.

## Неподдерживаемые флэш-устройства USB

---



**ОСТОРОЖНО!** Загрузка с помощью флэш-устройства USB может выполняться не на всех компьютерах. Если в служебной программе настройки компьютера (F10) указан порядок загрузки по умолчанию, предусматривающий, что попытка загрузки с флэш-устройства предшествует загрузке с жесткого диска, то загрузка данного компьютера с флэш-устройства USB возможна. В противном случае необходимо будет использовать загрузочную дискету.

---

Чтобы создать загрузочное флэш-устройство USB, необходимо иметь:

■ Компьютер одной из следующих моделей:

- ❑ настольный компьютер Compaq Evo D500 со сверхплоским горизонтальным корпусом;
- ❑ компьютер Compaq Evo D510 модернизируемая модель с вертикальным корпусом/с уменьшенным корпусом;
- ❑ профессиональные настольные компьютеры HP Compaq d530 следующих серий – со сверхплоским горизонтальным корпусом, с уменьшенным корпусом или модернизируемая модель с вертикальным корпусом;
- ❑ переносной компьютер Compaq Evo серий N400c, N410c, N600c, N610c, N620c, N800c или N1000c;
- ❑ переносной компьютер Compaq Presario серий 1500 или 2800.

В зависимости от индивидуальных особенностей системы BIOS будущие модели компьютеров также могут поддерживать загрузку с флэш-устройства USB.

---



**ОСТОРОЖНО!** Если используется модель компьютера, не указанная в приведенном выше списке, убедитесь, что в служебной программе настройки компьютера (F10) указан порядок загрузки по умолчанию, предусматривающий, что попытка загрузки с USB-устройства предшествует загрузке с жесткого диска.

---

- Загрузочную дискету DOS с программами FDISK и SYS. Если на ней отсутствует программа SYS, то может использоваться программа FORMAT, однако в этом случае все файлы, имеющиеся на устройстве Drive Key, будут утеряны.
- 1. Если на компьютере с подключенными накопителями SCSI, ATA RAID или SATA имеются платы PCI, отключите компьютер и отсоедините шнур питания.



**ОСТОРОЖНО!** Шнур питания ДОЛЖЕН БЫТЬ обязательно отсоединен.

- 2. Откройте корпус компьютера и удалите все платы PCI.
- 3. Подсоедините флэш-устройство USB к одному из USB-портов компьютера и отсоедините все другие USB-устройства хранения данных за исключением USB-накопителей гибких дискет. Закройте корпус компьютера.
- 4. Подсоедините шнур питания и включите компьютер. Как только индикатор монитора станет зеленым, нажмите клавишу **F10**, чтобы перейти к служебной программе настройки компьютера.
- 5. Выберите «Advanced/PCI devices» (дополнительные/PCI устройства), чтобы отключить контроллеры IDE и SATA. При отключении контроллера SATA запомните номер IRQ, назначенный этому контроллеру. Этот номер потребуется позднее назначить снова. Выйдите из программы настройки, подтвердив сделанные изменения.  
SATA IRQ: \_\_\_\_\_
- 6. Вставьте загрузочную дискету DOS с программами FDISK.COM и SYS.COM (или FORMAT.COM) в дисковод и включите компьютер, чтобы выполнить загрузку с загрузочной дискеты DOS.
- 7. Запустите программу FDISK и удалите все имеющиеся на флэш-устройстве USB разделы. Создайте новый раздел и пометьте его в качестве активного. Выйдите из программы FDISK, нажав клавишу **ESC**.

8. Если после выхода из программы FDISK не произойдет автоматической перезагрузки компьютера, нажмите клавиши **CTRL+ALT+DEL**, чтобы выполнить загрузку с дискеты DOS.
9. Введите после приглашения A:\ **FORMAT C: /S** и нажмите клавишу **ENTER**. Программа Format выполнит форматирование флэш-устройства USB, добавит системные файлы и предложит ввести метку тома.
10. Нажмите клавишу **ENTER**, чтобы отказаться от ввода метки или введите ее, если хотите это сделать.
11. Отключите компьютер и отсоедините шнур питания. Откройте корпус компьютера и снова установите удаленные ранее платы PCI. Закройте экран компьютера.
12. Подсоедините шнур питания, удалите дискету и включите компьютер.
13. Как только индикатор монитора станет зеленым, нажмите клавишу **F10**, чтобы перейти к служебной программе настройки компьютера.
14. Выберите «Advanced/PCI devices» (дополнительные/PCI устройства), чтобы снова включить контроллеры IDE и SATA, отключенные ранее на шаге 5. Назначьте контроллеру SATA, его исходный номер IRQ.
15. Сохраните изменения и выйдите из служебной программы. Компьютер загрузится с устройства флэш-устройства USB, которое отобразится в качестве диска C.



Порядок загрузки по умолчанию на различных компьютерах может быть разным, и может быть изменен с помощью служебной программы настройки компьютера (F10).

При использовании версии DOS из Windows 9x, некоторое время может отображаться экран с эмблемой Windows. Если это нежелательно, добавьте файл нулевого размера с именем LOGO.SYS в корневой каталог устройства Drive Key.

Далее см. [«Копирование на несколько компьютеров»](#) на стр. 15.

## Двухпозиционная кнопка питания

При включении интерфейса управления питанием (ACPI — Advanced Configuration and Power Interface) в Windows 2000, Windows NT Professional, Windows NT Home Edition и Windows XP кнопка питания может выполнять как функции включения и отключения питания, так и приостановки работы компьютера. Средство приостановки работы не производит полного отключения питания, а переводит компьютер в режим пониженного энергопотребления. Это позволяет быстро приостановить работу компьютера, не закрывая приложений, а затем так же быстро вернуться в исходный рабочий режим без потери данных.

Для изменения функций кнопки питания выполните следующие действия.

1. В Windows 2000 нажмите кнопку **Пуск**, затем последовательно выберите команды **Настройка, Панель управления и Электропитание**.  
В Windows XP нажмите кнопку **Пуск**, затем последовательно выберите **Панель управления, Производительность и обслуживание и Электропитание**.
2. В окне **Свойства: Электропитание** выберите вкладку **Дополнительно**.
3. В разделе **Кнопка питания** выберите необходимые параметры.

После установки функций кнопки питания для приостановки и возобновления работы для перевода компьютера в режим с очень низким потреблением энергии (режим ожидания) нажмите кнопку питания. Для быстрого возобновления работы компьютера повторно нажмите на кнопку питания. Для полного отключения подачи энергии нажмите и удерживайте кнопку питания в течение четырех секунд.



**ОСТОРОЖНО!** Используйте кнопку отключения питания компьютера, только если система не отвечает. Выключение питания компьютера без взаимодействия с операционной системой может привести к повреждению или потере данных на жестком диске.

## Узел Интернета

Для обеспечения высокой производительности, совместимости и надежности компьютеров Hewlett–Packard инженеры компании осуществляют строгий контроль и отладку программного обеспечения, разработанного компанией Hewlett–Packard и независимыми производителями, а также разрабатывают специальное программное обеспечение.

При переходе на новые или измененные операционные системы необходимо установить программное обеспечение поддержки, разработанное для соответствующей операционной системы. Если планируется использовать версию операционной системы Microsoft Windows, отличающуюся от версии, имеющейся на компьютере, для обеспечения правильной работы всех функций следует установить соответствующие драйверы устройств и служебные программы.

Компания Hewlett–Packard позаботилась о том, чтобы максимально упростить процесс поиска, получения, обновления и установки последних версий программного обеспечения поддержки. Программы можно загрузить с веб-узла <http://www.hp.com/support>.

На веб-узле имеются последние версии драйверов устройств, служебных программ и образы флэш-ПЗУ, необходимые для последней версии операционной системы Microsoft Windows, установленной на данном компьютере Hewlett–Packard.

## Объединения и партнеры

Предлагаемые компанией Hewlett–Packard решения по управлению интегрированы с другими приложениями управления компьютером и основываются на таких отраслевых стандартах, как:

- Desktop Management Interface (DMI, интерфейс управления настольным компьютером) 2.0
- Технология Wake on LAN
- Интерфейс ACPI
- SMBIOS
- Поддержку предзагрузочной среды выполнения (PXE)

## Средства отслеживания и защита

С помощью средств отслеживания (Asset Tracking), реализованных на данном компьютере, собираются данные для диспетчеров HP Insight Manager, HP Client Manager и для других приложений управления системой. Тесная автоматизированная связь между компонентами средств отслеживания и этими программными продуктами позволяет выбрать средство управления, которое наиболее подходит для данной информационно вычислительной среды и позволяет получить большую отдачу от сделанных вложений в программное обеспечение.

Компания Hewlett-Packard также предлагает различные решения для средств контроля доступа к важным компонентам компьютера и информации. Если установлено устройство встроенной защиты ProtectTools, оно предотвращает несанкционированный доступ к данным, проверяет целостность системы и выявляет попытки посторонних лиц получить доступ к системе. Средства защиты, такие как датчик снятия крышки и блокировка крышки, доступные на некоторых моделях, помогают предотвратить несанкционированный доступ к внутренним компонентам персонального компьютера. Деактивируя параллельный порт, последовательный порт, порт универсальной последовательной шины USB или способность загрузки сменных носителей, можно воспрепятствовать доступу к ценным информационным ресурсам. Сообщения об изменении памяти и предупреждения датчика снятия крышки могут автоматически передаваться приложениям управления системой для обеспечения оперативного уведомления о несанкционированном доступе к внутренним компонентам компьютера.




Такие средства защиты, как датчик снятия крышки и блокировка крышки имеется не на всех компьютерах.

Для управления параметрами защиты компьютеров Hewlett–Packard используйте следующие служебные программы:

- Служебные программы настройки компьютера используются для локального управления. Для получения дополнительных сведений и инструкций по использованию служебных программ по настройке компьютера см. *Руководство по настройке компьютера (F10)*, входящее в комплект поставки.
- Предлагаемые компанией Hewlett–Packard диспетчеры Client Manager и System Software Manager используются для удаленного управления. Это программное средство обеспечивает надежную и последовательную интеграцию и управление параметрами защиты с использованием простого компилятора командных строк.

В приведенной ниже таблице и последующих разделах объясняется, как локально управлять средствами защиты компьютера, используя служебные программы настройки компьютера (F10).

## Обзор средств защиты

Средство	Назначение	Установка
Управление загрузкой со съемных носителей	Предотвращает загрузку компьютера со съемных дисков (имеется на некоторых моделях).	Из меню служебных программ настройки компьютера (F10).
Управление последовательными, параллельными, инфракрасными и USB-портами	Предотвращает передачу данных через встроенный параллельный, последовательный, USB- или инфракрасный порт.	Из меню служебных программ настройки компьютера (F10).
 Дополнительные сведения о программе настройки компьютера см. в <i>Руководстве по настройке компьютера (F10)</i> . Поддерживаемый набор средств защиты может различаться в зависимости от конфигурации компьютера.		



**Обзор средств защиты** (Продолжение)

<b>Средство</b>	<b>Назначение</b>	<b>Установка</b>
Power-On Password (пароль на включение компьютера)	Препятствует работе на персональном компьютере до введения пароля. Действует как при начальном включении компьютера, так и при перезапуске.	Из меню служебных программ настройки компьютера (F10).
Setup Password (пароль настройки)	Предотвращает внесение изменений в конфигурацию компьютера (с помощью служебной программы настройки компьютера) без ввода пароля.	Из меню служебных программ настройки компьютера (F10).
Устройства встроенной защиты	Предотвращают с помощью шифрования и паролей несанкционированный доступ к данным. Проверяют целостность системы и выявляют попытки посторонних пользователей осуществить доступ к системе.	Из меню служебных программ настройки компьютера (F10).
DriveLock	Предотвращает несанкционированный доступ к данным на указанных жестких дисках MultiBay. Данное средство имеется не на всех моделях.	Из меню служебных программ настройки компьютера (F10).
 Дополнительные сведения о программе настройки компьютера см. в <i>Руководстве по настройке компьютера (F10)</i> . Поддерживаемый набор средств защиты может различаться в зависимости от конфигурации компьютера.		

**Обзор средств защиты** (Продолжение)

<b>Средство</b>	<b>Назначение</b>	<b>Установка</b>
датчик снятия крышки	Указывает, что была снята крышка или боковая панель компьютера. Может быть настроен на запрос ввода пароля на доступ к настройке для перезапуска компьютера, после того как были сняты крышка или боковая панель компьютера. Дополнительные сведения см. в <i>Справочном руководстве по работе с оборудованием</i> на компакт-диске <i>Библиотека документов</i> . Данное средство имеется не на всех моделях.	Из меню служебных программ настройки компьютера (F10).
Защита главной загрузочной записи	Может предотвращать несанкционированные или злонамеренные изменения главной загрузочной записи на текущем загрузочном диске, а также обеспечивает средства восстановления последней из MBR, не содержащей ошибок.	Из меню служебных программ настройки компьютера (F10).
Предупреждения об изменении памяти	Регистрирует добавление, перемещение или удаление модулей памяти и уведомляет об этом пользователя и системного администратора.	Сведения о включении предупреждений об изменении памяти находятся в электронном <i>Руководстве по системе управления компьютером</i> .
 Дополнительные сведения о программе настройки компьютера см. в <i>Руководстве по настройке компьютера (F10)</i> . Поддерживаемый набор средств защиты может различаться в зависимости от конфигурации компьютера.		

**Обзор средств защиты** (Продолжение)

<b>Средство</b>	<b>Назначение</b>	<b>Установка</b>
Дескриптор принадлежности	Выводит на экран во время инициализации системы (защищенной паролем на доступ к Setup) информацию о владельце, определенную системным администратором.	Из меню служебных программ настройки компьютера (F10).
Кабельное замковое устройство	Предотвращает доступ к внутренним компонентам компьютера во избежание нежелательных изменений конфигурации или удаления компонентов. Может использоваться также для крепления компьютера к неподвижному объекту для предотвращения его перемещения.	Используя замок с тросиком, прикрепите компьютер к неподвижному объекту.
Блокировочная скоба	Предотвращает доступ к внутренним компонентам компьютера во избежание нежелательных изменений конфигурации или удаления компонентов.	Установите запорное устройство на блокировочную скобу для предотвращения нежелательных изменений конфигурации или удаления компонентов.
 <p>Дополнительные сведения о программе настройки компьютера см. в <i>Руководстве по настройке компьютера (F10)</i>.</p> <p>Поддерживаемый набор средств защиты может различаться в зависимости от конфигурации компьютера.</p>		

## Защита паролем

Пароль, вводимый при включении питания и препятствующий несанкционированному использованию компьютера, будет затребован каждый раз при включении или повторной инициализации компьютера для дальнейшего доступа к его прикладным программам или содержащейся в его памяти информации. Пароль на доступ к программе настройки препятствует несанкционированному доступу непосредственно к программе настройки и может также использоваться для входа в компьютер вместо пароля, вводимого при включении питания. Таким образом, если вместо затребованного пароля, вводимого при включении питания, будет введен пароль на доступ к программе настройки, все равно будет получен доступ к компьютеру.

Пароль на доступ к программе настройки, действительный для всей сети, позволяет системному администратору зарегистрироваться на любом компьютере сети для проведения обслуживающих работ, не задавая пароля на включение компьютера, даже если таковой был установлен в данной системе.

## Установка пароля на доступ к программе настройки компьютера с помощью программы настройки компьютера

Если компьютер оснащен устройством встроенной защиты, см. [«Встроенная защита» на стр. 38](#).

Установка пароля на доступ к программе настройки с помощью программы настройки компьютера предотвращает изменение его конфигурации (использование служебной программы настройки (F10)) без ввода пароля.

1. Включите или перезагрузите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузить компьютер**.
2. Как только индикатор монитора станет зеленым, нажмите клавишу **F10**. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.



Если не нажать клавишу **F10** в нужное время, придется выключать компьютер, потом включать его снова и повторно нажимать клавишу **F10**, чтобы получить доступ к программе.

3. Выберите пункт **Security** (защита), затем — **Setup Password** (пароль настройки) и следуйте инструкциям на экране.
4. Перед выходом из программы выберите команду **File** (файл), затем — **Save Changes and Exit** (сохранить изменения и выйти).

## Использование пароля на включение питания

### Программа настройки компьютера

Установка пароля на включение питания с помощью программы настройки компьютера предотвращает доступ к компьютеру непосредственно при включении питания, пока не будет введен пароль. После того как пароль установлен, программа настройки компьютера отображает команду Password Options (параметры пароля) в меню Security (Безопасность). Для параметра пароля можно выбрать значение «Password Prompt on Warm Boot» (запрос пароля при перезагрузке). При включенном запросе на ввод пароля при перезагрузке пароль должен также вводиться при каждой перезагрузке компьютера.

1. Включите или перезагрузите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузить компьютер**.
2. Как только индикатор монитора станет зеленым, нажмите клавишу **F10**. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.



Если не нажать клавишу **F10** в нужное время, придется выключать компьютер, потом включать его снова и повторно нажимать клавишу **F10**, чтобы получить доступ к программе.

3. Выберите пункт **Security** (защита), затем — команду **Power-On Password** (пароль на включение компьютера) и следуйте инструкциям на экране.
4. Перед выходом из программы выберите команду **File** (файл), затем — **Save Changes and Exit** (сохранить изменения и выйти).

## Ввод пароля на включение питания

Для ввода пароля на включение питания выполните следующие действия.

1. Включите или перезагрузите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузить компьютер**.
2. Когда на экране монитора появится значок ключа, введите текущий пароль и нажмите клавишу **ENTER**.



Вводите пароль внимательно, так как в целях безопасности вводимые буквенные и цифровые знаки не отображаются на экране.

Если пароль введен неправильно, на экране появится значок сломанного ключа. Попробуйте еще раз. По истечении трех неудачных попыток ввода пароля для продолжения придется выключить и снова включить компьютер.

## Ввод пароля для настройки компьютера

Если компьютер оснащен устройством встроенной защиты, см. [«Встроенная защита» на стр. 38](#).

Если для компьютера был задан пароль настройки, каждый раз при запуске программы настройки на экране будет появляться запрос на ввод пароля настройки.

1. Включите или перезагрузите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузить компьютер**.
2. Как только индикатор монитора станет зеленым, нажмите клавишу **F10**.



Если не нажать клавишу **F10** в нужное время, придется выключать компьютер, потом включать его снова и повторно нажимать клавишу **F10**, чтобы получить доступ к программе.

3. Когда на экране монитора появится значок ключа, введите пароль настройки и нажмите клавишу **ENTER**.



Вводите пароль внимательно, так как в целях безопасности вводимые буквенные и цифровые знаки не отображаются на экране.

Если пароль введен неправильно, на экране появится значок сломанного ключа. Попробуйте еще раз. По истечении трех неудачных попыток ввода пароля для продолжения придется выключить и снова включить компьютер.

## Изменение пароля на включение питания или входа в программу настройки

Если компьютер оснащен устройством встроенной защиты, см. [«Встроенная защита» на стр. 38](#).

1. Включите или перезапустите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузить компьютер**. Для изменения пароля настройки запустите программу **Computer Setup** (настройка компьютера).
2. При появлении значка ключа введите текущий пароль, косую черту (/) или альтернативный разделитель, затем введите новый пароль, еще одну косую черту (/) или альтернативный разделитель и еще раз новый пароль в следующем порядке:  
**текущий пароль/новый пароль/новый пароль**



Вводите пароль внимательно; так как в целях безопасности вводимые знаки не отображаются на экране.

3. Нажмите клавишу **ENTER**.

Новый пароль действует с момента следующего включения компьютера.



См. «Национальные разделительные символы клавиатуры» на стр. 37 для получения сведений по альтернативным разделителям. Пароль на включение питания и пароль настройки можно также изменять, используя параметры защиты программы настройки компьютера.

---

## Удаление пароля на включение питания или пароля настройки

Если компьютер оснащен устройством встроенной защиты, см. «Встроенная защита» на стр. 38.

1. Включите или перезапустите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузка**. Для удаления пароля настройки запустите программу **Computer Setup** (настройка компьютера).
2. При появлении значка ключа введите текущий пароль, а затем косую черту или альтернативный разделитель, как показано ниже: **текущий пароль/**
3. Нажмите клавишу **ENTER**.



См. «Национальные разделительные символы клавиатуры» для получения сведений по альтернативным разделителям. Пароль на включение питания и пароль настройки можно также изменять, используя параметры защиты программы настройки компьютера.

---



## Национальные разделительные символы клавиатуры

Каждая клавиатура разрабатывается в соответствии с конкретными требованиями соответствующей страны. Символы и знаки препинания, которые используются для изменения или удаления пароля, зависят от клавиатуры, которая поставляется вместе с компьютером.

### Национальные символы-разделители, используемые на клавиатуре

ВНСУ*	-	Испанский	-	Словацкий	-
Арабский	/	Итальянский	-	США	/
				(английский язык)	
Бельгийский	=	Канадский	é	Тайваньский	/
		(французский язык)			
Бразильский	/	Китайский	/	Тайский	/
Великобританский	/	Корейский	/	Турецкий	.
Венгерский	-	Латинская Америка	-	Французский	!
Германский	-	Норвежский	-	Чешский	-
Греческий	-	Польский	-	Шведский/Финский	/
Датский	-	Португальский	-	Швейцарский	-
Иврит	.	Русский	/	Японский	/

\* Для Боснии-Герцеговины, Хорватии, Словении и Югославии

## Сброс паролей

Если вы забыли свой пароль, доступ к компьютеру будет закрыт. Для получения информации по процедуре сброса паролей обратитесь к *Руководству по устранению неполадок*.

Если компьютер оснащен устройством встроенной защиты, см. [«Встроенная защита»](#).

## Встроенная защита

Устройство встроенной защиты ProtectTools объединяет в себе защиту с помощью шифрования и пароля в целях обеспечения повышенной защиты для шифрованных файлов и папок файловой системе EFS (Embedded File System) и обеспечения безопасности электронной почты при использовании приложения Microsoft Outlook и Outlook Express. Средство ProtectTools доступно на некоторых профессиональных настольных компьютерах как параметр Configured-To-Order (CTO). Это средство предназначено для тех клиентов компании Hewlett-Packard, которые в первую очередь заинтересованы в обеспечении безопасности данных: несанкционированный доступ к данным представляет для них собой гораздо более серьезную опасность, чем их простая потеря. В средстве ProtectTools используются следующие четыре пароля:

- «(F10) Setup» (настройка (F10)) — чтобы войти в программу настройки компьютера (F10) и включить/отключить средство ProtectTools
- «Take Ownership» (право собственности) — должен устанавливаться и использоваться системным администратором, предоставляющим права пользователям и задающим параметры безопасности
- «Emergency Recovery Token» (маркер аварийного восстановления) — должен устанавливаться системным администратором, разрешает восстановление в случае выхода из строя компьютера или чипа ProtectTools
- «Basic User» (основной пользователь) — устанавливается и применяется конечным пользователем.



---

В случае утери пароля конечного пользователя, шифрованные данные восстановить невозможно. Поэтому, можно безопасно использовать ProtectTools, только скопировав данные с жесткого диска в корпоративную информационную систему или регулярно создавая резервные копии.

---

Устройство встроенной защиты ProtectTools представляет собой защитный чип, отвечающий стандарту TCSP 1.1, который дополнительно устанавливается на системную плату некоторых профессиональных настольных компьютеров. Каждый защитный чип устройства встроенной защиты ProtectTools является уникальным и совместим только с конкретным компьютером. Каждый защитный чип реализует основные функции защиты независимо от других компонентов компьютера (таких как процессор, память ил операционная система).

Компьютер, поддерживающий устройство встроенной защиты ProtectTools, обладает дополнительной и более высокой степенью защиты по сравнению с возможностями, которые обеспечиваются операционными системами Microsoft Windows 2000, Windows XP Professional или Windows XP Home Edition. Например, если операционная система может шифровать файлы и папки с помощью средств EFS, то устройство встроенной защиты ProtectTools предоставляет дополнительный уровень защиты посредством создания ключей шифрования на основе корневого ключа платформы (хранящегося в кремниевой микросхеме). Данный процесс известен под названием «сплетение» ключей шифрования. Средство ProtectTools не может предотвратить доступ по сети к компьютеру без использования ProtectTools.

Основные возможности устройства встроенной защиты ProtectTools обеспечивают:

- проверку подлинности платформы
- защищенное хранение
- целостность данных

---

**ОСТОРОЖНО!** защиту паролей **Доступ к шифрованным данным не может быть получен без ввода соответствующих паролей.**

---

## Настройка паролей

### Программа настройки компьютера

Пароль настройки может быть создан, а устройство встроенной защиты может быть включено с помощью служебной программы настройки компьютера F10.

1. Как только индикатор монитора станет зеленым, нажмите клавишу **F10**.



Если не нажать клавишу **F10** в нужное время, придется выключать компьютер, потом включать его снова и повторно нажимать клавишу **F10**, чтобы получить доступ к программе.

2. С помощью клавиши **СТРЕЛКА ВВЕРХ** или **СТРЕЛКА ВНИЗ** выберите язык, затем нажмите клавишу **ENTER**.
3. С помощью клавиши **СТРЕЛКА ВЛЕВО** или **СТРЕЛКА ВПРАВО** переместитесь на вкладку **Security** (защита), а затем с помощью клавиши **СТРЕЛКА ВВЕРХ** или **СТРЕЛКА ВНИЗ** выберите **Setup Password** (пароль настройки). Нажмите клавишу **ENTER**.
4. Введите и подтвердите пароль. Нажмите клавишу **F10**, чтобы принять пароль.



Вводите пароль внимательно; так как в целях безопасности вводимые знаки не отображаются на экране.

5. С помощью клавиши **СТРЕЛКА ВВЕРХ** или **СТРЕЛКА ВНИЗ** выберите **Embedded Security Device** (устройство встроенной защиты). Нажмите клавишу **ENTER**.
6. Если в диалоговом окне будет выбрано значение **Embedded Security Device — Disable** (устройство встроенной защиты — отключено), измените его с помощью клавиши **СТРЕЛКА ВЛЕВО** или **СТРЕЛКА ВПРАВО** на **Embedded Security Device — Enable** (устройство встроенной защиты — включено). Нажмите клавишу **F10**, чтобы принять изменения.



**ОСТОРОЖНО!** При выборе **Reset to Factory Settings — Reset** (возврат к стандартным настройкам — сброс), все ключи будут очищены и зашифрованные данные восстановить окажется невозможно, за исключением случая, когда эти ключи ранее были заархивированы (см. «Право собственника и маркер аварийного восстановления»). Следует выбрать только **Reset** (сброс), если будет предложено это сделать при выполнении процедуры восстановления зашифрованных данных (см. «Восстановление зашифрованных данных» на стр. 44).

7. С помощью клавиши **СТРЕЛКА ВЛЕВО** или **СТРЕЛКА ВПРАВО** выберите **File** (файл). С помощью клавиши **СТРЕЛКА ВВЕРХ** или **СТРЕЛКА ВНИЗ** выберите **Save Changes and Exit** (сохранить изменения и выйти). Нажмите клавишу **ENTER**, затем нажмите клавишу **F10**, чтобы подтвердить внесенные изменения.

## Право собственника и маркер аварийного восстановления

Пароль Take Ownership (право собственника) используется для включения или отключения платформы защиты и авторизации пользователей. Если устройство встроенной защиты выйдет из строя, механизм аварийного восстановления представит возможность осуществлять авторизацию пользователей и доступ к данным.

1. Если используется Windows XP Professional или Windows XP Home Edition, нажмите кнопку **Пуск** и выберите последовательно команды **Все программы**, **HP ProtectTools Embedded Security Tools** (устройство встроенной защиты HP ProtectTools), **Embedded Security Initialization Wizard** (мастер инициализации встроенной защиты).

Если используется Windows 2000, нажмите кнопку **Пуск** и выберите последовательно **Программы**, **HP ProtectTools Embedded Security Tools** (устройство встроенной защиты HP ProtectTools), **Embedded Security Initialization Wizard** (мастер инициализации встроенной защиты).

2. Нажмите кнопку **Next** (далее).

3. Введите и подтвердите пароль Take Ownership (право собственника) и нажмите кнопку **Next** (далее).



Вводите пароль внимательно; так как в целях безопасности вводимые знаки не отображаются на экране.

4. Нажмите кнопку **Next** (далее), чтобы принять местоположение архива восстановления.
5. Введите и подтвердите пароль Emergency Recovery Token (маркер аварийного восстановления), затем нажмите кнопку **Next** (далее).
6. Вставьте дискету, на которой будет сохранен ключ маркера аварийного восстановления (Emergency Recovery Token Key). Нажмите кнопку **Browse** (просмотр) и выберите эту дискету.



**ОСТОРОЖНО!** Ключ маркера аварийного восстановления используется для восстановления зашифрованных данных в случае выхода из строя компьютера или чипа встроенной защиты.  
**Восстановить данные без такого ключа невозможно.**  
(Доступ к данным по-прежнему может быть осуществлен только с использованием пароля основного пользователя (Basic User)).  
Храните эту дискету в надежном месте.

7. Нажмите кнопку **Save** (сохранить), чтобы принять местоположение и имя файла по умолчанию, после чего нажмите кнопку **Next** (далее).
8. Нажмите кнопку **Next** (далее), чтобы подтвердить введенные значения настроек перед тем, как будет инициализирована платформа защиты.



На экран может быть выведено сообщение о том, что функция встроенной защиты не включена. Щелкать это сообщение не следует; его обработка при выполнении описываемой процедуры будет проведена через несколько секунд, после чего данное сообщение закроется.

9. Нажмите кнопку **Next** (далее), чтобы пропустить настройку местных политик.

10. Убедитесь, что установлен флажок Start Embedded Security User Initialization Wizard (запустить мастер инициализации пользователя встроенной защиты), затем нажмите кнопку **Finish** (готово).

После этого автоматически запустится мастер инициализации пользователя.

### основной пользователь

В процессе инициализации пользователя будет создан пароль основного пользователя (Basic User Password). Этот пароль необходим для ввода зашифрованных данных и осуществления доступа к ним.



**ОСТОРОЖНО!** Пароль основного пользователя должен надежно храниться. **Осуществить доступ к зашифрованным данным без этого пароля невозможно.**

1. Если мастер инициализации пользователя не откроется:

Если используется Windows XP Professional или Windows XP Home Edition, нажмите кнопку **Пуск** и выберите последовательно команды **Все программы, HP ProtectTools Embedded Security Tools** (устройство встроенной защиты HP ProtectTools), **User Initialization Wizard** (мастер инициализации пользователя).

Если используется Windows 2000, нажмите кнопку **Пуск** и выберите последовательно **Программы, HP ProtectTools Embedded Security Tools** (устройство встроенной защиты HP ProtectTools), **User Initialization Wizard** (мастер инициализации пользователя).

2. Нажмите кнопку **Next** (далее).
3. Введите и подтвердите ключ пароля основного пользователя (Basic User Key), затем нажмите кнопку **Next** (далее).



Вводите пароль внимательно; так как в целях безопасности вводимые знаки не отображаются на экране.

4. Нажмите кнопку **Next** (далее), чтобы подтвердить введенные значения настроек.
5. Выберите соответствующие функции защиты и нажмите кнопку **Next** (далее).
6. Выберите соответствующего клиента электронной почты, а затем нажмите кнопку **Next** (далее).
7. Нажмите кнопку **Next** (далее), чтобы применить сертификат шифрования.
8. Нажмите кнопку **Next** (далее), чтобы подтвердить введенные значения настроек.
9. Нажмите кнопку **Готово**.
10. Перезагрузите компьютер.

## Восстановление шифрованных данных

Чтобы восстановить данные после замены чипа ProtectTools, необходимо иметь:

- файл SPemRecToken.xml, содержит ключ маркера аварийного восстановления;
  - файл SPemRecArchive.xml, содержит сведения о местоположении скрытой папки: C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\Recovery Archive
  - Пароли ProtectTools
    - ☐ «Setup» (настройка)
    - ☐ «Take Ownership» (право собственника)
    - ☐ «Emergency Recovery Token» (маркер аварийного восстановления)
    - ☐ «Basic User» (основной пользователь)
1. Перезагрузите компьютер.
  2. Как только индикатор монитора станет зеленым, нажмите клавишу **F10**.





Если не нажать клавишу **F10** в нужное время, придется выключать компьютер, потом включать его снова и повторно нажимать клавишу **F10**, чтобы получить доступ к программе.

3. Введите пароль настройки, затем нажмите клавишу **ENTER**.
4. С помощью клавиши **СТРЕЛКА ВВЕРХ** или **СТРЕЛКА ВНИЗ** выберите язык, а затем нажмите клавишу **ENTER**.
5. С помощью клавиши **СТРЕЛКА ВЛЕВО** или **СТРЕЛКА ВПРАВО** перейдите на вкладку **Security** (защита), а затем с помощью клавиши **СТРЕЛКА ВЛЕВО** или **СТРЕЛКА ВПРАВО** выберите **Embedded Security Device** (устройство встроенной защиты). Нажмите клавишу **ENTER**.
6. Если для выбора будет доступна только одна возможность, **Embedded Security Device — Disable**, (устройство встроенной защиты — отключено):
  - a. С помощью клавиши **СТРЕЛКА ВЛЕВО** или **СТРЕЛКА ВПРАВО** измените его на **Embedded Security Device — Enable** (устройство встроенной защиты — включено). Нажмите клавишу **F10**, чтобы принять производственное изменение.
  - b. С помощью клавиши **СТРЕЛКА ВЛЕВО** или **СТРЕЛКА ВПРАВО** переместитесь к параметру **File** (файл). С помощью клавиши **СТРЕЛКА ВВЕРХ** или **СТРЕЛКА ВНИЗ** переместитесь к кнопке **Save Changes and Exit** (сохранить изменения и выйти). Нажмите клавишу **ENTER**, затем нажмите клавишу **F10**, чтобы подтвердить выбор.
  - c. Перейдите к шагу 1.

Если для выбора будут доступны две возможности, переходите к шагу 7.
7. С помощью клавиши **СТРЕЛКА ВВЕРХ** или **СТРЕЛКА ВНИЗ** переместитесь к параметру **Reset to Factory Settings — Do Not Reset** (возврат к стандартным настройкам — не сбрасывать). Нажмите клавишу **СТРЕЛКА ВЛЕВО** или **СТРЕЛКА ВПРАВО** один раз.

На экран будет выведено сообщение, в котором говорится о том, что выполнение данного действия, приведет к возврату настройки параметров устройства встроенной защиты к стандартным настройкам, если эти параметры будут сохранены при выходе. Нажмите любую клавишу, чтобы продолжить процедуру.

Нажмите клавишу **ENTER**.

8. После этого выбранным будет являться значение **Reset to Factory Settings — Reset** (возврат к стандартным настройкам — сброс). Нажмите клавишу **F10**, чтобы принять производственное изменение.
9. С помощью клавиши СТРЕЛКА ВЛЕВО или СТРЕЛКА ВПРАВО переместитесь к параметру **File** (файл). С помощью клавиши СТРЕЛКА ВВЕРХ или СТРЕЛКА ВНИЗ переместитесь к кнопке **Save Changes and Exit** (сохранить изменения и выйти). Нажмите клавишу **ENTER**, затем нажмите клавишу **F10**, чтобы подтвердить выбор.
10. Перезагрузите компьютер.
11. Как только индикатор монитора станет зеленым, нажмите клавишу **F10**.



---

Если не нажать клавишу **F10** в нужное время, придется выключать компьютер, потом включать его снова и повторно нажимать клавишу **F10**, чтобы получить доступ к программе.

---

12. Введите пароль «Setup» (настройка), затем нажмите клавишу **ENTER**.
13. С помощью клавиши СТРЕЛКА ВВЕРХ или СТРЕЛКА ВНИЗ выберите язык, а затем нажмите клавишу **ENTER**.
14. С помощью клавиши СТРЕЛКА ВЛЕВО или СТРЕЛКА ВПРАВО переместитесь на вкладку the **Security** (защита), затем с помощью клавиши СТРЕЛКА ВЛЕВО или СТРЕЛКА ВПРАВО выберите **Embedded Security Device** (устройство встроенной защиты). Нажмите клавишу **ENTER**.

15. Если в диалоговом окне будет выбрано значение **Embedded Security Device — Disable** (устройство встроенной защиты — отключено), с помощью клавиши **СТРЕЛКА ВЛЕВО** или **СТРЕЛКА ВПРАВО** измените его на **Embedded Security Device — Enable** (устройство встроенной защиты — включено). Нажмите клавишу **F10**.
16. С помощью клавиши **СТРЕЛКА ВЛЕВО** или **СТРЕЛКА ВПРАВО** переместитесь к параметру **File** (файл). С помощью клавиши **СТРЕЛКА ВВЕРХ** или **СТРЕЛКА ВНИЗ** переместитесь к кнопке **Save Changes and Exit** (сохранить изменения и выйти). Нажмите клавишу **ENTER**, затем нажмите клавишу **F10**, чтобы подтвердить выбор.
17. After Windows opens:

Если используется Windows XP Professional или Windows XP Home Edition, нажмите кнопку **Пуск** и выберите последовательно команды **Все программы, HP ProtectTools Embedded Security Tools** (средство встроенной защиты HP ProtectTools), **Embedded Security Initialization Wizard** (мастер инициализации встроенной защиты).

Если используется Windows 2000, нажмите кнопку **Пуск** и выберите последовательно **Программы, HP ProtectTools Embedded Security Tools** (средство встроенной защиты HP ProtectTools), **Embedded Security Initialization Wizard** (мастер инициализации встроенной защиты).

18. Нажмите кнопку **Next** (далее).
19. Введите и подтвердите пароль Take Ownership (право собственника). Нажмите кнопку **Next** (далее).



Вводите пароль внимательно; так как в целях безопасности вводимые знаки не отображаются на экране.

20. Убедитесь, что выбран параметр «Create a new recovery archive» (создать новый архив восстановления). В разделе **Recovery archive location**, (местоположение архив восстановления) нажмите кнопку **Browse** (просмотр).

21. Не принимайте имя файла по умолчанию. Введите новое имя файла, чтобы избежать перезаписи исходного файла.
22. Нажмите кнопку **Save** (сохранить), а затем кнопку **Next** (далее).
23. Введите и подтвердите пароль Emergency Recovery Token (маркер аварийного восстановления), затем нажмите кнопку **Next** (далее).
24. Вставьте дискету, на которой будет сохранен ключ маркера аварийного восстановления. Нажмите кнопку **Browse** (просмотр) и выберите эту дискету.
25. Не принимайте имя ключа по умолчанию. Введите новое имя ключа, чтобы избежать перезаписи исходного ключа.
26. Нажмите кнопку **Save** (сохранить), а затем кнопку **Next** (далее).
27. Нажмите кнопку **Next** (далее), чтобы подтвердить указанные настройки перед тем, как будет инициализирована платформа защиты.



---

На экран может быть выведено сообщение о том, что ключ основного пользователя не может быть загружен. Щелкать это сообщение не следует; его обработка при выполнении описываемой процедуры будет проведена через несколько секунд, после чего данное сообщение закроется.

---

28. Нажмите кнопку **Next** (далее), чтобы пропустить настройку местных политик.
29. Снимите флажок **Start Embedded Security User Initialization Wizard** (запустить мастер инициализации пользователя встроенной защиты). Нажмите кнопку **Готово**.
30. Щелкните правой кнопкой мыши значок ProtectTools на панели инструментов и выберите команду **Initialize Embedded Security restoration** (восстановить инициализацию встроенной защиты).

Это приведет к запуску мастера «HP ProtectTools Embedded Security Initialization Wizard» (мастер инициализации встроенной защиты HP ProtectTools).

31. Нажмите кнопку **Next** (далее).
32. Вставьте дискету, на которой хранится исходный ключ маркера аварийного восстановления. Нажмите кнопку **Browse** (просмотр), затем определите местоположение маркера и дважды щелкните его, чтобы ввести в поле. По умолчанию им является A:\SPEmRecToken.xml.
33. Введите исходный пароль Token и нажмите кнопку **Next** (далее).
34. Нажмите кнопку **Browse** (просмотр), затем дважды щелкните исходный архив восстановления, чтобы ввести его имя в поле. По умолчанию им является C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\RecoveryArchive\SPEmRecArchive.xml.
35. Нажмите кнопку **Next** (далее).
36. Щелкните компьютер, данные которого требуется восстановить, а затем нажмите кнопку **Next** (далее).
37. Нажмите кнопку **Next** (далее), чтобы подтвердить введенные значения.
38. Если мастер сообщит, что платформа защиты восстановлена, переходите к шагу 39.  
  
Если мастер сообщит, что восстановление выполнить не удалось, возвращайтесь к шагу 10. Ввод паролей, местоположения и имени маркера, местоположения и имени архива должен осуществляться очень внимательно.
39. Нажмите кнопку «Finish» (готово).
40. Если используется Windows XP Professional или Windows XP Home Edition, нажмите кнопку **Пуск** и выберите последовательно команды **Все программы**, **HP ProtectTools Embedded Security Tools** (средство встроенной защиты HP ProtectTools), **User Initialization Wizard** (мастер инициализации пользователя).  
  
Если используется Windows 2000, нажмите кнопку **Пуск** и выберите последовательно **Программы**, **HP ProtectTools Embedded Security Tools** (средство встроенной защиты HP ProtectTools), **User Initialization Wizard** (мастер инициализации пользователя).

41. Нажмите кнопку **Next** (далее).
42. Выберите **Recover your basic user key** (восстановить ключ основного пользователя) и нажмите кнопку **Next** (далее).
43. Выберите пользователя, введите исходный пароль Basic User Key (ключ основного пользователя), и нажмите кнопку **Next** (далее).
44. Нажмите кнопку **Next** (далее), чтобы подтвердить введенные значения параметров и принять местоположение восстановления данных по умолчанию.



---

Шаги с 45 по 49 позволяют повторно установить исходную конфигурацию основного пользователя.

---

45. Выберите соответствующую функцию защиты и нажмите кнопку **Next** (далее).
46. Выберите соответствующего клиента электронной почты, а затем нажмите кнопку **Next** (далее).
47. Выберите сертификат шифрования и нажмите кнопку **Next** (далее), чтобы применить его.
48. Нажмите кнопку **Next** (далее), чтобы подтвердить введенные значения настроек.
49. Нажмите кнопку **Готово**.
50. Перезагрузите компьютер.



---

**ОСТОРОЖНО!** Пароль основного пользователя должен надежно храниться. **Осуществить доступ к шифрованным данным без этого пароля невозможно.**

---

## DriveLock

Блокировка дисков (DriveLock) — это предусмотренное отраслевым стандартом средство защиты, которое предотвращает несанкционированный доступ к данным на определенных жестких дисках. Блокировка дисков включена в качестве дополнительного средства в программу настройки компьютера. Это средство доступно только в случае обнаружения жестких дисков, поддерживающих функцию DriveLock.

Средство блокировки дисков предназначено для тех клиентов компании Hewlett–Packard, которые в первую очередь заинтересованы в обеспечении безопасности данных. Для таких клиентов затраты на жесткий диск и на восстановление хранимых на нем данных несопоставимы с тем уроном, который они могут понести в случае несанкционированного доступа к содержимому диска. Чтобы, с одной стороны, обеспечить безопасность такого уровня, а с другой стороны, дать приемлемое решение в случае, когда забыт пароль, в средстве блокировки применяется схема с использованием двух паролей. Один пароль должен быть установлен и использован системным администратором, а другой обычно устанавливается и используется конечным пользователем. Однако если оба пароля забыты, нет никакой возможности разблокировать диск. Поэтому, можно безопасно использовать блокировку диска, только скопировав данные с жесткого диска в корпоративную информационную систему или регулярно создавая резервные копии.

В случае утраты паролей блокировки диска жесткий диск непригоден для дальнейшего использования. Для тех пользователей, которые не относятся к описанной выше категории клиентов, это может оказаться неоправданным риском. Для тех же пользователей, кто относится к упомянутой категории, такой риск может быть вполне сопоставим с характером данных, хранимых на жестком диске.

## Использование функции DriveLock

Параметр DriveLock (блокировка диска) содержится в меню Security (защита) программы настройки компьютера. Здесь имеется ряд параметров, позволяющих устанавливать главный пароль и включать защиту диска. Чтобы включить блокировку диска, необходим пользовательский пароль. Поскольку начальная конфигурация блокировки диска обычно выполняется системным администратором, главный пароль должен быть установлен первым. Компания Hewlett-Packard рекомендует системным администраторам устанавливать главный пароль в любом случае: собираются они или нет включить блокировку диска. Это даст системным администраторам возможность изменять параметры блокировки диска, если они намереваются заблокировать диск впоследствии. Как только установлен главный пароль, системный администратор может включить блокировку диска или оставить ее отключенной.

Если в системе имеется заблокированный жесткий диск, в ходе проверки POST будет запрошен пароль для снятия блокировки устройства. Если был установлен пароль на включение компьютера и он соответствует пользовательскому паролю на разблокировку устройства, в ходе проверки POST не будет запрашиваться ввод пароля. В противном случае пользователь должен будет ввести пароль блокировки диска. Может использоваться как главный, так и пользовательский пароль. У пользователя есть две попытки для ввода правильного пароля. Если ни одна из попыток не будет успешной, проверка POST будет продолжена, но диск останется недоступным.



## Приложения блокировки диска

Лучше всего использовать средства защиты жесткого диска в корпоративной среде, где системный администратор обеспечивает пользователям возможность использовать жесткие диски Multibay на некоторых компьютерах. Системный администратор отвечает за конфигурацию жестких дисков Multibay, для которых, помимо всего прочего, будет установлен главный пароль блокировки диска. В случае, если пользователь забудет пользовательский пароль или оборудование будет передано другому сотруднику, всегда можно использовать главный пароль для переустановки пользовательского пароля и получения доступа к жесткому диску.


Компания Hewlett–Packard рекомендует тем системным администраторам, которые решили включить блокировку диска, разработать также корпоративную политику по установке и эксплуатации главных паролей. Это необходимо для того, чтобы предотвратить возникновения ситуаций, когда сотрудники намеренно или непреднамеренно устанавливают оба пароля на блокировку диска перед тем, как уйти из компании. В таких случаях жесткий диск окажется полностью непригодным к использованию, и его придется заменить. Аналогично при отсутствии главного пароля системные администраторы могут оказаться лишены доступа к жесткому диску и не смогут выполнять обычную проверку наличия несанкционированного программного обеспечения, а также другие функции по контролю и поддержке.

Пользователям, у которых нет особых требований к безопасности данных, компания Hewlett–Packard не рекомендует включать блокировку диска. К этой категории относятся частные пользователи и те пользователи, которые, как правило, не держат на жестком диске секретные данные. Для этих пользователей потенциальная потеря жесткого диска в случае, если они забудут оба пароля, значит гораздо больше, чем те данные, для защиты которых предназначено средство блокировки диска. Доступ к программе настройки и средству блокировки диска может быть закрыт с помощью пароля настройки. Задав пароль настройки и не сообщая его пользователям, системные администраторы могут предотвратить включение пользователями блокировки диска.

## Датчик снятия крышки

Датчик снятия крышки (Smart Cover Sensor), имеющийся на некоторых моделях, использует аппаратные и программные средства, которые позволяют предупреждать о снятии крышки или боковой панели компьютера. Существует три уровня защиты, описанные в следующей таблице.

### Уровни защиты датчика снятия крышки

Уровень	Параметр	Описание
Уровень 0	Disabled (Отключен)	Датчик снятия крышки отключен (по умолчанию).
Уровень 1	Notify User (уведомление пользователя)	Во время перезагрузки компьютера на экране отображается сообщение о том, что была снята крышка или боковая панель компьютера.
Уровень 2	Setup Password (пароль настройки)	Во время перезагрузки компьютера на экране отображается сообщение о том, что была снята крышка или боковая панель компьютера. Необходимо ввести пароль настройки, чтобы продолжить.
 Данные параметры могут быть изменены с помощью программы настройки компьютера. Дополнительные сведения о программе настройки компьютера см. в <i>Руководстве по настройке компьютера (F10)</i> .		

## Настройка уровня защиты датчика снятия крышки

Чтобы установить уровень защиты датчика снятия крышки, выполните следующие действия.

1. Включите или перезагрузите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузить компьютер**.
2. Как только индикатор монитора станет зеленым, нажмите клавишу **F10**. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.



Если не нажать клавишу **F10** в нужное время, придется выключать компьютер, потом включать его снова и повторно нажимать клавишу **F10**, чтобы получить доступ к программе.

3. Выберите команду **Security** (защита), затем — **Smart Cover** (крышка) и следуйте инструкциям на экране.
4. Перед выходом из программы выберите команду **File** (файл), затем — **Save Changes and Exit** (сохранить изменения и выйти).

## Блокировка крышки

Блокировка крышки компьютера (Smart Cover Lock) представляет собой замок, имеющийся на некоторых компьютерах Hewlett–Packard, управляемый программными средствами. Эта блокировка предотвращает несанкционированный доступ к внутренним компонентам. Компьютер поставляется со снятой блокировкой Smart Cover Lock.



**ОСТОРОЖНО!** Для обеспечения максимального уровня блокировки крышки убедитесь, что установлен пароль для входа в программу настройки компьютера. Пароль настройки предотвращает несанкционированный доступ к служебной программе настройки компьютера.



Блокировка крышки имеется не на всех компьютерах.

## Включение блокировки крышки.

Чтобы активировать и включить блокировку крышки, выполните следующие шаги.

1. Включите или перезагрузите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузить компьютер**.
2. Как только индикатор монитора станет зеленым, нажмите клавишу **F10**. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.



Если не нажать клавишу **F10** в нужное время, придется выключать компьютер, потом включать его снова и повторно нажимать клавишу **F10**, чтобы получить доступ к программе.

3. Выберите команду **Security** (защита), затем — **Smart Cover** (блокировка крышки) и установите параметр **Locked** (включена).
4. Перед выходом из программы выберите команду **File** (файл), затем — **Save Changes and Exit** (сохранить изменения и выйти).

## Выключение блокировки крышки.

1. Включите или перезапустите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузить компьютер**.
2. Как только индикатор монитора станет зеленым, нажмите клавишу **F10**. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.



Если не нажать клавишу **F10** в нужное время, придется выключать компьютер, потом включать его снова и повторно нажимать клавишу **F10**, чтобы получить доступ к программе.

3. Выберите команду **Security** (защита), затем — **Smart Cover** (блокировка крышки) и установите параметр **Unlocked** (отключена).

4. Перед выходом из программы выберите пункт **File** (файл), затем — **Save Changes and Exit** (сохранить изменения и выйти).

## Дополнительный ключ блокировки крышки

Если при включенной блокировке крышки (Smart Cover Lock) ввод пароля для разблокирования невозможен, для открытия крышки компьютера необходим аварийный ключ FailSafe. Этот ключ может потребоваться в следующих ситуациях.

- Отключение электроэнергии
- Сбой при запуске
- Сбой компонента компьютера (например, процессора или блока питания)
- Забыт пароль



**ОСТОРОЖНО!** Дополнительный ключ является специальным инструментом, поставляемым компанией Hewlett-Packard. Рекомендуется заказать этот ключ заблаговременно у поставщика услуг или уполномоченного представителя.

Для получения ключа выполните одно из следующих действий.

- Обратитесь к уполномоченному представителю Hewlett-Packard или поставщику услуг.
- Обратитесь по телефону (список телефонных номеров содержится в документе о предоставлении гарантии).

Дополнительные сведения об использовании дополнительного ключа блокировки крышки см. в *Справочном руководстве по работе с оборудованием*.

## Защита главной загрузочной записи

Главная загрузочная запись (MBR — Master Boot Record) содержит сведения, необходимые для успешной загрузки диска и доступа к данным, которые на нем хранятся. Средство защиты главной загрузочной записи позволяет предотвратить несанкционированные или умышленные изменения MBR, которые могут быть вызваны компьютерными вирусами или неправильным использованием некоторых служебных программ. Оно также позволяет восстанавливать последнюю не содержавшую ошибок запись MBR, в случае обнаружения изменений в MBR при перезапуске компьютера.

Чтобы включить защиту MBR, выполните следующие шаги.

1. Включите или перезагрузите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузить компьютер**.
2. Как только индикатор монитора станет зеленым, нажмите клавишу **F10**. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.



---

Если не нажать клавишу **F10** в нужное время, придется выключать компьютер, потом включать его снова и повторно нажимать клавишу **F10**, чтобы получить доступ к программе.

---

3. Выберите команду **Security** (защита), затем — **Master Boot Record Security** (защита главной загрузочной записи) и установите вариант **Enabled** (включено).
4. Выберите команду **Security** (защита), затем — **Save Master Boot Record** (сохранить главную загрузочную запись).
5. Перед выходом из программы выберите команду **File** (файл), затем — **Save Changes and Exit** (сохранить изменения и выйти).

При включенной защите MBR BIOS предотвращает любые изменения, которые производятся в MBR на текущем загрузочном диске в MS-DOS или в режиме Windows Safe Mode.



В большинстве операционных систем контролируется доступ к MBR на текущем загрузочном диске; BIOS не позволяет предотвратить изменения, которые могут произойти при запуске операционной системы.

При каждом включении или перезагрузке компьютера BIOS сравнивает MBR текущего загрузочного диска с копией, сохраненной ранее. Если будут найдены изменения или текущий загрузочный диск не тот, на котором была сохранена предыдущая MBR, отобразится следующее сообщение:

1999—Master Boot Record has changed  
(1999 — главная загрузочная запись изменилась).

Нажмите любую клавишу для входа в программу настройки и настройки защиты MBR.

После входа в программу настройки компьютера необходимо выполнить следующие действия:

- сохранить MBR текущего загрузочного диска;
- восстановить ранее сохраненную MBR; или
- отключить средство защиты MBR.

Для этого необходимо знать пароль на доступ к программе настройки (если он был установлен).

Если будут найдены изменения или текущий загрузочный диск **не** тот, на котором была сохранена предыдущая MBR, отобразится следующее сообщение:

Master Boot Record Hard Drive has changed  
(2000 — главная загрузочная запись жесткого диска изменилась).

Нажмите любую клавишу для входа в программу настройки и настройки защиты MBR.

После входа в программу настройки компьютера необходимо выполнить следующие действия:

- сохранить MBR текущего загрузочного диска; или
- отключить средство защиты MBR.

Для этого необходимо знать пароль на доступ к программе настройки (если он был установлен).

В том случае, если ранее сохраненная MBR была повреждена, отобразится следующее сообщение:

1998—Master Boot Record has been lost  
(1998 — главная загрузочная запись утеряна).

Нажмите любую клавишу для входа в программу настройки и настройки защиты MBR.

После входа в программу настройки компьютера необходимо выполнить следующие действия:

- сохранить MBR текущего загрузочного диска; или
- отключить средство защиты MBR.

Для этого необходимо знать пароль на доступ к программе настройки (если он был установлен).

## **Действия, необходимые перед созданием разделов и форматированием текущего загрузочного диска**

Убедитесь, что отключена защита MBR, прежде чем изменять разбиение или форматировать текущий загрузочный диск. Некоторые служебные программы для работы с дисками, такие как FDISK и FORMAT, обновляют MBR. Если защита MBR включена, при изменении разбиения или форматировании диска могут появляться сообщения об ошибках служебной программы или предупреждения средства защиты MBR при следующем включении или перезагрузке компьютера. Чтобы включить защиту MBR, выполните следующие шаги.

1. Включите или перезагрузите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузить компьютер**.



2. Как только индикатор монитора станет зеленым, нажмите клавишу **F10**. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.



Если не нажать клавишу **F10** в нужное время, придется выключать компьютер, потом включать его снова и повторно нажимать клавишу **F10**, чтобы получить доступ к программе.

3. Выберите команду **Security** (защита), затем — **Master Boot Record Security** (защита главной загрузочной записи) и установите вариант **Disabled** (отключено).
4. Перед выходом из программы выберите команду **File** (файл), затем — **Save Changes and Exit** (сохранить изменения и выйти).

## Кабельное замковое устройство

На задней панели некоторых моделей компьютеров имеется запорный узел, позволяющий физически закрепить компьютер на рабочем месте.

Наглядно проиллюстрированные инструкции см. в *Справочном руководстве по работе с оборудованием* на компакт-диске *Справочная библиотека*.

## Технология идентификации по отпечаткам пальцев

Устраняя необходимость ввода паролей конечными пользователями, технология идентификации по отпечаткам пальцев (HP Fingerprint Identification Technology) повышает сетевую безопасность, упрощает процедуру входа в систему и снижает затраты на управление корпоративными компьютерными сетями. Доступная по цене, эта технология предназначена не только для организаций, использующих высокие технологии и имеющих повышенный уровень секретности.



Поддержка технологии идентификации по отпечаткам пальцев варьируется в зависимости от модели.

Дополнительные сведения см. на веб-узле:

<http://h18000.www1.hp.com/solutions/security>.

## Средства уведомления о сбоях и восстановления

Средства уведомления о сбоях и восстановления совмещают передовые аппаратные и программные технологии и позволяют предотвратить потерю важных данных и свести к минимуму время вынужденного простоя оборудования.

При возникновении сбоя на экране компьютера отображается предупреждающее сообщение с описанием сбоя и рекомендуемых действий. Затем можно ознакомиться с текущим состоянием системы с помощью диспетчера HP Client Manager. Если компьютер подключен к сети, управляемой с помощью программ HPInsight Manager, HP Client Manager или других программ управления компьютерами, уведомление о сбое отправляется также приложению управления сетью.

## Система защиты диска

Система защиты диска (DPS, Drive Protection System) — это диагностическое средство, встроенное в жесткие диски некоторых настольных компьютеров Hewlett–Packard. Система DPS предназначена для обнаружения неполадок, которые могут привести к негарантийной замене жесткого диска.

При изготовлении компьютеров Hewlett–Packard каждый устанавливаемый жесткий диск проверяется с использованием DPS, и на него записываются специальные нестираемые данные. При каждом применении DPS результаты проверки записываются на жесткий диск. Службы технической службы могут использовать эти данные для определения причины запуска проверки DPS. Сведения по использованию средств DPS содержатся в *Руководстве по устранению неполадок*.

## **Помехозащищенный блок питания**

Встроенный помехозащищенный блок питания обеспечивает повышение надежности работы компьютера при наличии помех в сети питания. Этот блок питания выдерживает импульсные помехи амплитудой до 2000 вольт без каких-либо сбоев в работе компьютера или потери данных.

## **Датчик температуры**

Датчик температуры представляет собой программное средство и компонент оборудования, который следит за внутренней температурой компьютера. Он выводит на экран предупреждение о том, что превышен температурный предел, что позволяет предпринять необходимые действия, прежде чем будут повреждены внутренние компоненты компьютера или утрачены данные.

---

# Указатель

## A-Z

ActiveUpdate 9

Altiris 6

Altiris PC Transplant Pro 7

DiskOnKey

*см. также* HP Drive Key

загрузочное устройство 18 – 24

Drivelock 51 – 53

HP Client Manager 5

HP Drive Key

*см. также* DiskOnKey

загрузочное устройство 18 – 24

Multibay, защита 51 – 53

PCN (Proactive Change Notification) 8

Proactive Change Notification (PCN) 8

ProtectTools, встроенная защита

Emergency Recovery Key (ключ  
аварийного восстановл.) 41

аварийное восстановление 44 – 50

пароли

Basic User (основной  
пользователь) 43

Emergency Recovery Token (маркер  
аварийного восстановл.) 41

Take Ownership (право  
собственника) 41

ProtectTools, устройство встроенной  
защиты 38 – 50

пароли

программа настройки 40

PXE — предзагрузочная среда  
выполнения 4

Remote ROM Flash 10

Smart Cover Lock 55 – 57

Smart Cover Sensor 54

SSM (System Software Manager) 8

System Software Manager (SSM) 8

## A

аварийное восстановление,

ProtectTools 44 – 50

аварийный загрузочный блок ПЗУ 12

адреса URL (веб-узлы). *см.* веб-узлы

## Б

безопасность

блокировка крышки 55

дополнительный ключ 57

защита ПЗУ 10

параметры, установка 27

средства защиты, таблица 28

блок питания, помехозащищенный 63

блокировка крышки 55

включение 56

выключение 56

блокировка крышки, безопасность 55

блокировка крышки, заказ

дополнительного ключа 57

## **В**

### ввод

- включение компьютера, пароль 34
- пароль настройки 34

### веб-узлы

- ActiveUpdate 9
- Altiris 7
- Altiris PC Transplant Pro 7
- HP Client Manager 5
- HPQFlash 11
- PC deployment 3
- Proactive Change Notification 8
- ROMPaq, образы 10
- System Software Manager (SSM) 8
- программное обеспечение,
  - поддержка 26
- репликация, служебная
  - программа 17
- технология идентификации по
  - отпечаткам пальцев 61
- удаленное изменение данных
  - флэш-ПЗУ 11
  - Флэш-ПЗУ 10

### включение блокировки крышки 56

- включение компьютера, пароль
  - ввод 34
  - изменение 35

### включение питания, пароль

- удаление 36

### внутри корпуса компьютера,

- температура 63

### восстановление системы 11

### восстановление шифрованных

- данных 44 – 50

### восстановление, программное

- обеспечение 3

### встроенная защита 38 – 50

### выключение блокировки крышки 56

## **Г**

- главная загрузочная запись,
  - защита 58 – 60

## **Д**

### датчик снятия крышки

- настройка 55
- уровни защиты 54

### две функции кнопки питания 25

### диагностические средства для жестких

- дисков 62

### диск, защита 62

### диск, клонирование 3

### дополнительный ключ

- безопасность 57
- заказ 57

### доступ к компьютеру, контроль 27

## **Ж**

### жесткие диски, диагностические

- средства 62

## **З**

### загрузочное устройство

- DiskOnKey 18 – 24
- HP Drive Key 18 – 24
- дискета 17
- создание 17 – 24
- флэш-устройство USB 18 – 24

### загрузочный диск, важная

- информация 60

### заказ дополнительного ключа 57

### замок с тросиком 61

### защита

- DriveLock 51 – 53
- MultiBay 51 – 53
- Smart Cover Lock 55 – 57
- Smart Cover Sensor 54
- пароль 32
- средство ProtectTools 38 – 50

защита главная загрузочная

запись 58 – 60

защита жестких дисков 62

защита ПЗУ, безопасность 10

## И

изменение настройки программного обеспечения 3

изменение операционных систем, важная информация 26

изменение пароля 35

изменения, уведомление об 8

индикаторы клавиатуры, ПЗУ, таблица 13

Интернет–адреса, см. веб–узлы

исходная конфигурация настроек репликация 14

## К

клавиатура, национальные разделительные символы 37

кнопка питания

настройка 25

кнопка питания с двумя функциями 25

контроль доступа к компьютеру 27

## Н

настройка

начальная 2

настройка кнопки питания 25

национальная клавиатура, разделительные символы 37

начальная конфигурация 2

## О

обновление ПЗУ 10

образ программного обеспечения 3

операционные системы, важная информация 26

## П

пароль

ProtectTools 40 – 44

включение компьютера 34

защита 32

изменение 35

настройка 32

настройки 34

сброс 37

удаление 36

пароль на настройку

изменение 35

пароль настройки

ProtectTools 40

ввод 34

задание 32

удаление 36

ПЗУ

индикаторы клавиатуры, таблица 13

повреждение 12

удаленное изменение данных

флэш–ПЗУ 10

ПЗУ, обновление 10

повреждение системного ПЗУ 12

помехозащищенный блок питания 63

предзагрузочная среда

выполнения (PXE) 4

программное обеспечение

Remote ROM Flash 10

System Software Manager 8

аварийный загрузочный блок

ПЗУ 12

восстановление 3

главная загрузочная запись, защита 58 – 60

интеграция 3

обновление нескольких компьютеров 8

система защиты дисков 62  
служебные программы копирования  
    исходных настроек компьютера 14  
средства отслеживания 27  
уведомление о сбоях и  
    восстановление 62  
удаленная установка системы 4

## **Р**

разбиение диска на разделы,  
    важная информация 60  
разделительные символы, таблица 37

## **С**

сброс пароля 37  
система, восстановление 11  
Служебные программы копирования  
    исходных настроек компьютера 14  
средства клонирования,  
    программное обеспечение 3  
средства отслеживания 27

средства развертывания, программное  
    обеспечение 3

## **Т**

температура внутри компьютера 63  
температурный датчик 63  
технология идентификации по  
    отпечаткам пальцев 61

## **У**

уведомление о сбоях 62  
уведомление об изменениях 8  
удаление пароля 36  
удаленная установка 4  
удаленная установка системы, доступ 4

## **Ф**

флэш-устройство USB,  
    загрузочное 18 – 24  
форматирование диска,  
    важная информация 60